(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－55731

(43)公開日　平成９年(1997)２月25日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ　9/18			Ｈ０４Ｌ　9/00	６５１	
Ｇ０９Ｃ　1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６６０Ｄ	
Ｇ１１Ｂ　20/10		7736－5Ｄ	Ｇ１１Ｂ　20/10	Ｈ	
// Ｇ０６Ｆ　12/14	３２０		Ｇ０６Ｆ　12/14	３２０Ｂ	

審査請求　未請求　請求項の数15　ＯＬ　（全　７　頁）

(21)出願番号　特願平7－206351

(22)出願日　平成７年(1995)８月11日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　佐古　曜一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　栗原　章
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　弁理士　小池　晃　（外２名）

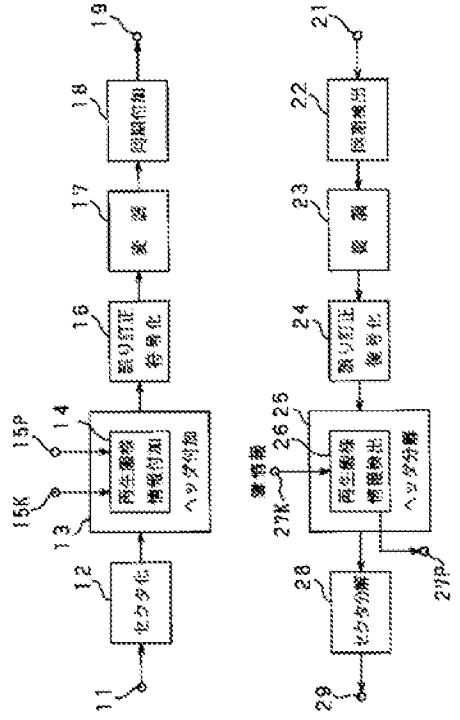
最終頁に続く

(54)【発明の名称】　信号伝送方法、信号記録媒体及び信号再生装置

(57)【要約】

【課題】　コピー管理情報や課金情報等の再生態様情報の改変や改竄を防止し、不正使用や不法コピーを防止する。

【解決手段】　ヘッダ付加回路１３内の再生態様情報付加回路１４により、端子１５Ｐからのコピー管理情報や課金情報等の再生態様情報に対して、端子１５Ｋからの鍵情報に応じて暗号化のためのデータ変換を施し、データに付加して伝送する。再生側では、ヘッダ分離回路２５内の再生態様情報検出回路２６により、暗号化された再生態様情報を、端子２７Ｋからの鍵情報を用いて暗号復号化のためのデータ変換を施し、元の再生態様情報を端子２７Ｐより取り出す。



【特許請求の範囲】
【請求項１】　入力信号に再生態様情報を付加して伝送する信号伝送方法において、
上記再生態様情報に対して暗号化の鍵情報に応じたデータ変換を施すことを特徴とする信号伝送方法。
【請求項２】　上記再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むことを特徴とする請求項１記載の信号伝送方法。
【請求項３】　上記データ変換は、上記再生態様情報のデータと暗号化の鍵情報との論理演算により行われることを特徴とする請求項１記載の信号伝送方法。
【請求項４】　上記暗号化の鍵情報は、アドレス情報を少なくとも一部に含むことを特徴とする請求項１記載の信号伝送方法。
【請求項５】　上記再生態様情報は、所定の位置指定情報により指定される位置に配置されることを特徴とする請求項１記載の信号伝送方法。
【請求項６】　入力信号に再生態様情報を付加して伝送する信号伝送方法において、
上記再生態様情報を所定の位置指定情報により指定される位置に配置することを特徴とする信号伝送方法。
【請求項７】　上記再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むことを特徴とする請求項６記載の信号伝送方法。
【請求項８】　入力信号に付加される再生態様情報に対して暗号化の鍵情報に応じたデータ変換を施して得られた信号が記録されて成ることを特徴とする信号記録媒体。
【請求項９】　上記再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むことを特徴とする請求項８記載の信号記録媒体。
【請求項１０】　上記再生態様情報は、所定の位置指定情報により指定される位置に配置されることを特徴とする請求項８記載の信号記録媒体。
【請求項１１】　入力信号に付加される再生態様情報が所定の位置指定情報により指定された位置に配置されて記録されて成ることを特徴とする信号記録媒体。
【請求項１２】　入力信号に付加される再生態様情報に対して暗号化の鍵情報に応じたデータ変換を施して記録された信号を再生する信号再生装置であって、
上記暗号化の鍵情報を入力する鍵情報入力手段と、
この鍵情報入力手段からの鍵情報に応じて上記暗号化に対応する復号化のためのデータ変換を施す手段とを有することを特徴とする信号再生装置。
【請求項１３】　上記再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むことを特徴とする請求項１２記載の信号再生装置。
【請求項１４】　上記再生態様情報は、所定の位置指定情報により指定される位置に配置されることを特徴とする請求項１２記載の信号再生装置。
【請求項１５】　入力信号に付加される再生態様情報が所定の位置指定情報により指定された位置に配置されて記録されて信号を再生する信号再生装置であって、
上記位置指定情報により指定された位置の再生態様情報を取り出す手段を有することを特徴とする信号再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、伝送あるいは記録再生される信号のコピー防止や不正使用の阻止、あるいは課金システムに適用可能な信号伝送方法、信号記録媒体、及び信号再生装置に関する。
【０００２】
【従来の技術】近年において、光ディスク等のディジタル記録媒体の大容量化と普及により、コピー防止や不正使用の阻止が重要とされてきている。すなわち、ディジタルオーディオデータやディジタルビデオデータの場合には、コピーあるいはダビングにより劣化のない複製物を容易に生成でき、また、コンピュータデータの場合には、元のデータと同一のデータが容易にコピーできるため、既に不法コピーによる著作権の侵害等の弊害が生じてきているのか実情である。
【０００３】このようなことから、上記不法コピーの防止を目的として、オリジナルのデータ記録媒体に、不法コピー防止のための情報を記録するような規格が提案され用いられている。
【０００４】例えば、いわゆるＲ－ＤＡＴ（Rotary head Digital Audio Taperecoder ）と称されるディジタルオーディオ信号記録再生装置における上記不法コピー防止のための方式としては、信号記録媒体としてのディジタルオーディオテープ上に記録されるディジタルオーディオ信号のメインデータエリアに、ディジタルコピーの禁止や段階的な世代コピーを禁止（すなわち世代制限）するための禁止コード（いわゆるＳＣＭＳ：シリアルコピー管理システムの規格の禁止コード）を記録しておき、ディジタルオーディオ信号記録装置がこの禁止コードを検出したときに、新たなディジタルオーディオテープ上への当該ディジタルオーディオ信号のコピー記録を禁止するような方式が採用されている。
【０００５】また、信号記録媒体に記録された例えばディジタルビデオ信号の不法コピーを防止するために、上記Ｒ－ＤＡＴにおける記録再生装置間での不法コピー防止の方式と同様に、オリジナルのディジタル記録媒体に不法コピー防止のための所定のＩＤビット（ＣＧＭＳ：コピー世代管理システムの規格の禁止コード）を記録することが考えられている。
【０００６】さらに、コンピュータデータの場合には、ファイル内容自体を暗号化鍵情報を用いて暗号化し、それを正規の登録された使用者にのみ使用許諾することが行われている。なおこれは、情報流通の形態として、情

報が暗号化されて記録されたディジタル記録媒体を配布しておき、使用者が必要とした内容について料金を払って鍵情報を入手し、暗号を解いて利用可能とするようなシステムに結び付くものである。

【０００７】

【発明が解決しようとする課題】ところが、上述したような従来の信号記録媒体用の禁止コードや暗号鍵情報等は、特開平５－１７３８９１号公報に示されるように、記録媒体上のユーザからアクセスされるシステム固有の特定の場所に記録されている。

【０００８】また、コピー管理情報や課金情報等の再生態様情報は、データの記録媒体上の位置やビットアロケーションが決定されているため、読み飛ばしたり、改竄して使用したりするという不正使用の問題がある。すなわち、コピー管理情報や課金情報等の再生態様情報は、例えばユーザからアクセス可能な場所にあるため、悪意のあるユーザによる解読や不法コピーの対象になりやすかった。

【０００９】また、上記再生態様情報の配置がそれぞれの暗号化手法において任意の場所で固定的であると、互換性がなくなる虞れがある。また、再生態様情報を固定的に配置すれば、暗号化の手法も固定化されることになり、柔軟性，拡張性に乏しく、フォーマット自身の寿命を縮めてしまう可能性がある。

【００１０】これは、ディジタル信号の記録再生や送受信等の伝送を行う場合のみならず、アナログ信号を伝送する場合にも問題とされることである。

【００１１】本発明は上述したような実情に鑑みてなされたものであり、コピー管理情報や課金情報等の再生態様情報を改変したり改竄したりすることによる不正使用や不法コピー等を困難にするような信号伝送方法、信号記録媒体及び信号再生装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】上記の課題を解決するために、本発明は、伝送あるいは記録しようとする信号に付加される再生態様情報に対して、暗号化の鍵情報に応じたデータ変換を施すことを特徴としている。

【００１３】ここで、再生態様情報は、コピー管理情報及び課金情報の少なくとも一方を含むものであり、この再生態様情報を所定の位置指定情報により指定される位置に配置することが好ましい。

【００１４】また、本発明は、再生態様情報を所定の位置指定情報により指定される位置に配置することを特徴としている。

【００１５】暗号化された再生態様情報は、鍵情報がなければ内容がわからないため、改変や改竄を受けにくい。また、位置指定情報によって指定された位置に再生態様情報を配置することで、容易に取り出せなくする。

【００１６】

【発明の実施の形態】以下、本発明の好ましい実施の形態について図面を参照しながら説明する。

【００１７】図１は、本発明の実施の形態が適用される構成の一例を概略的に示すブロック図である。この図１において、入力端子１１には、例えばアナログのオーディオ信号やビデオ信号をディジタル変換して得られたデータやコンピュータデータ等のディジタルデータが供給されている。この入力ディジタルデータは、セクタ化回路１２に送られ、所定データ量単位、例えば２０４８バイト単位でセクタ化される。セクタ化されたデータは、ヘッダ付加回路１３に送られて、各セクタの先頭に配置されるヘッダデータが付加される。このヘッダデータは、後述するように再生態様情報を含んでおり、この再生態様情報は、コピー管理情報と課金情報との少なくとも一方を有している。元のあるいはオリジナルの再生態様情報は、再生態様情報付加回路１４の端子１５Ｐに供給されており、この再生態様情報付加回路１４は、端子１５Ｋからの鍵情報に応じて上記元の再生態様情報に対して暗号化のためのデータ変換を施し、変換された再生態様情報を付加するようにしている。ヘッダ付加回路１３からのデータは誤り訂正符号化回路１６に送られ、この誤り訂正符号化回路１６では、データ遅延及びパリティ計算を行ってパリティを付加する。次の変調回路１７では、所定の変調方式に従って、例えば８ビットデータを１６チャンネルビットの変調データに変換し、同期付加回路１８に送る。同期付加回路１８では、上記所定の変調方式の変調規則を破る、いわゆるアウトオブルールのパターンの同期信号を所定のデータ量単位で付加し、出力端子１９を介して取り出している。

【００１８】出力端子１９からの出力信号は、例えば記録ヘッドに送ってディスク状やテープ状あるいは半導体等のデータ記録媒体に記録したり、通信媒体を介して送信したりすることにより伝送される。伝送された信号は、例えば再生ヘッドにより記録媒体から再生されたり、通信媒体を介して受信されたりして、再生側の入力端子２１に供給される。この入力端子２１に供給される信号は、伝送による信号劣化等を無視すれば出力端子１９から出力される信号と同じものである。

【００１９】入力端子２１からの信号は、同期検出回路２２に送られて、上記同期付加回路１８で付加された同期信号の分離が行われる。同期検出回路２２からのディジタル信号は、復調回路２３に送られて、上記変調回路１７の変調を復調する処理が行われる。具体的には、１６チャンネルビットを８ビットのデータに変換するような処理である。復調回路２３からのディジタルデータは、誤り訂正復号化回路２４に送られて、上記誤り訂正符号化回路１６での符号化の逆処理としての復号化処理が施される。誤り訂正復号化されたデータは、ヘッダ分離回路２５に送られて各セクタの先頭部分のヘッダが分離される。このヘッダデータ中の再生態様情報は、上述

したように鍵情報を用いた暗号化のデータ変換が施されており、再生態様情報検出回路２６により、端子２７Ｋからの鍵情報を用いて暗号復号化のためのデータ変換を施し、復号化された再生態様情報を端子２７Ｐより取り出すようにしている。ヘッダ分離回路２５によりヘッダが分離された残りのデータ、いわゆるユーザデータは、セクタ分解回路２８に送られて上記所定データ量単位のセクタに分解され、出力端子２９より取り出される。

【００２０】ここで、図2は、セクタフォーマットの具体例を示しており、１セクタは、２０４８バイトのユーザデータ領域４１に対して、４バイトの同期領域４２と、１６バイトのヘッダ領域４３と、４バイトの誤り検出符号（ＥＤＣ）領域４４とが付加されて構成されている。誤り検出符号領域４４の誤り検出符号は、ユーザデータ領域４１及びヘッダ領域４３に対して生成される３２ビットすなわち４バイトのＣＲＣ符号から成っている。ヘッダ領域４３内には、いわゆる巡回符号であるＣＲＣ４５、再生態様情報４６、多層ディスクのどの層かを示す層（レイヤ）４７、アドレス４８、予備４９の各領域が設けられている。

【００２１】再生態様情報４６は、例えば、１バイト（８ビット）で、図3に示すような構造を有している。この図3において、８ビットの再生態様情報は、上位側４ビットの課金情報５１と、下位側４ビットのコピー管理情報５２とから成っている。課金情報５１としては、当該セクタを含むファイルあるいはプログラムが、無料（フリー）であるか、視聴するための代金が必要（pay per view）であるか、コピーするための代金が必要（pay per copy）であるか等を示すコードやフラグが挙げられる。４ビットのコピー管理情報５２は、さらに２ビットのコピー世代情報５３と２ビットのコピー許可／禁止情報５４とに分割されている。２ビットのコピー世代情報５３としては、例えば“00”がオリジナル、“01”がコピーの１世代目、“10”がコピーの２世代目、“11”が３世代目以上のコピーをそれぞれ表し、２ビットのコピー許可／禁止情報５４としては、例えば、“00”がコピーフリー、“01”が２世代までコピーが可能、“10”が１世代のみコピーが可能、“11”がコピー禁止をそれぞれ表している。

【００２２】データを伝送する際、例えば記録したり送信したりする際には、上記課金情報５１やコピー管理情報５２から成る元のあるいはオリジナルの再生態様情報をそのまま用いずに、所定の鍵情報に応じた暗号化処理を施して、この暗号化された再生態様情報を上記セクタヘッダ領域４３の所定位置すなわち再生態様情報４６の位置に配置するようにしている。

【００２３】図４は、８ビットの再生態様情報に対して８ビットの鍵情報を用いて暗号化のためのデータ変換を施す一具体例を示す図である。すなわち、この図４の入力端子６１には上記元のあるいはオリジナルの再生態様情報が供給され、入力端子６２には８ビットの鍵情報が供給されている。これらの８ビットのデータは、ExOR（排他的論理和）回路６３に送られて各ビット毎に排他的論理和がとられ、８ビットの暗号化された再生態様情報となって出力端子６４より取り出される。

【００２４】このように、鍵情報を用いた暗号化処理を施すことにより、鍵情報がなければ元の再生態様情報の内容がわからず、内容の改変や改竄等の不法行為を有効に防止できる。

【００２５】また図５は、鍵情報のみならず、さらに８ビットのアドレス情報、例えばセクタアドレスの下位側１バイトを用いて暗号化のためのデータ変換を施す例を示している。すなわち、この図５の例では、入力端子６５に上記元のあるいはオリジナルの再生態様情報が供給され、入力端子６６に８ビットの鍵情報が供給されると共に、入力端子６７にセクタアドレスの下位側１バイト（８ビット）が供給されている。これらの３種類の８ビットデータは、ExOR（排他的論理和）回路６８に送られて対応する各ビット毎に排他的論理和がとられ、８ビットの暗号化された再生態様情報となって出力端子６９より取り出される。

【００２６】このように、セクタアドレスの一部を暗号化のためのデータ変換に用いることにより、セクタ毎に暗号化された再生態様情報が変化し、さらに改竄や不正使用の防止効果が高められる。

【００２７】なお、暗号化のためのデータ変換は、これらの図４、図５の例に限定されず、例えばいわゆるM系列の擬似乱数を用いて変換をかけてもよく、また、ExOR（排他的論理和）回路の代わりに、ＡＮＤ、ＯＲ、ＥｘＯＲ、ＮＡＮＤ、ＮＯＲ、インバート回路やこれらの組み合わせ回路等による論理演算を行わせてもよい。また論理演算以外に、データの位置を変える転置や、データの値を置き換える置換等も上記データ変換として使用できる。

【００２８】次に、図６は、記録媒体の一例としての光ディスク等のディスク状記録媒体１０１を示している。このディスク状記録媒体１０１は、中央にセンタ孔１０２を有しており、このディスク状記録媒体１０１の内周から外周に向かって、プログラム管理領域であるＴＯＣ（table of contents ）領域となるリードイン（leadin ）領域１０３と、プログラムデータが記録されたプログラム領域１０４と、プログラム終了領域、いわゆるリードアウト（lead out）領域１０５とが形成されている。オーディオ信号やビデオ信号再生用光ディスクにおいては、上記プログラム領域１０４にオーディオやビデオデータが記録され、このオーディオやビデオデータの時間情報等が上記リードイン領域１０３で管理される。

【００２９】上記鍵情報の一部として、データ記録領域であるプログラム領域１０４以外の領域に書き込まれた識別情報等を用いることが挙げられる。具体的には、Ｔ

ＯＣ領域であるリードイン領域１０３や、リードアウト領域１０５に、識別情報、例えば媒体固有の製造番号等の識別情報、製造元識別情報、販売者識別情報、あるいは、記録装置やエンコーダの固有の識別情報、カッティングマシンやスタンパ等の媒体製造装置の固有の識別情報を書き込むようにする。再生時には、上記識別情報を、暗号を復号するための鍵情報として用いるようにすればよい。また、リードイン領域１０３よりも内側に、物理的あるいは化学的に識別情報を書き込むようにし、これを再生時に読み取って、暗号を復号するための鍵情報として用いるようにしてもよい。

【００３０】また、上記再生態様情報を、記録位置を固定せずに任意の位置に記録するようにし、上記リードイン領域１０３のＴＯＣ領域のような所定領域に、上記再生態様情報の記録位置を指定するための位置指定情報を書き込んでおくことが挙げられる。この場合、ＴＯＣ領域の位置指定情報で直接的に上記再生態様情報の記録位置を指定してもよく、また、ＴＯＣ領域の位置指定情報ではデータ中のポインタが指定され、このポインタによって上記再生態様情報の記録位置を指定するようにしてもよい。

【００３１】すなわち、図７は、ＴＯＣデータ領域７１内の位置指定情報としてのポインタ７２により再生態様情報の記録位置を指示する例を示している。この図７において、再生態様情報の記録位置指定用のポインタ７１は、セクタアドレス情報７３、オフセット情報７４、バイト数情報７５及び属性情報から成っている。このようなポインタ７１のセクタアドレス情報７３により所定のセクタ７６が指定され、このセクタ７６内での再生態様情報７７のオフセット、すなわちセクタの先頭位置から再生態様情報７７までのバイト数がオフセット情報７４により指定され、この再生態様情報７７自体のバイト数がバイト数情報７５により指定される。

【００３２】このように、再生態様情報の記録位置が固定されないため、記録位置が固定されていることにより同じ位置からコピー管理情報等の再生態様情報が抜き出されて改変されるような事態を、有効に防止することができる。

【００３３】この再生態様情報は、上述したように鍵情報やアドレス等を用いた暗号化のためのデータ変換が施されているものであるが、このようなデータ変換を施さない元のあるいはオリジナルの再生態様情報を用いてもよい。

【００３４】また、ポインタのセクタアドレスやオフセット等に、販売元識別番号、製造者識別番号、記録装置識別番号等を用いるようにしてもよい。

【００３５】以上はディジタルデータ信号の伝送を行う場合の例であるが、本発明をアナログ信号の伝送に適用することもできる。

【００３６】すなわち、図８は、アナログビデオ信号に再生態様情報、特にコピー管理情報が付加された例を示している。

【００３７】この図８において、アナログビデオ信号の垂直帰線消去期間の所定の水平期間に、いわゆるプロテクトコード信号８１を混合している。このプロテクトコード信号８１を配置する水平期間は、例えば奇数フィールドでは２０Ｈ目（Ｈは水平期間）、偶数フィールドでは２８３Ｈ目である。このプロテクトコード信号８１は、例えば１４ビットのデータ８２と６ビットの誤り検出符号（ＣＲＣＣ）８３とから成っており、１４ビットのデータ８２内の６ビットのヘッダ８４に続く８ビットのデータ８５が上記再生態様情報、特にコピー管理情報を示すものであり、上述したように鍵情報を用いて暗号化処理が施されている。

【００３８】ここで、８ビットの再生態様情報を示すデータ８５の内容の具体例としては、ＭＳＢ（最上位ビット）８６がコピー禁止“１”／許可“０”を表し、次の２ビット８７がコピー世代、すなわち例えば“００”がオリジナル、“０１”がコピーの１世代目、“１０”がコピーの２世代目、“１１”が３世代目以上のコピーをそれぞれ表し、下位側の４ビット８８が機器のカテゴリコードを表している。

【００３９】このようなビデオ信号の再生態様情報の場合にも、暗号化を施しておくことにより、鍵情報がなければ内容がわからず、内容の改変を防止できる。

【００４０】なお、本発明は、上述した実施の形態の例のみに限定されるものではなく、例えば、記録媒体に対する記録／再生への適用のみならず、一般にディジタル信号やアナログ信号の伝送に適用することができることは勿論である。また、再生態様情報は上記具体例に限定されず、ビット数や内容を種々変更可能であり、また、ソースの内容やコピー履歴等の情報も含めるようにしてもよい。この他、本発明の要旨を逸脱しない範囲で種々の変更が可能である。

【００４１】

【発明の効果】本発明によれば、伝送あるいは記録しようとする信号に付加される再生態様情報に対して、暗号化の鍵情報に応じたデータ変換を施しているため、鍵情報がなければ内容がわからず、改変や改竄を防止でき、不正聴取や不法コピー等を有効に防止できる。

【００４２】さらに、暗号化された再生態様情報を所定の位置指定情報により指定される位置に配置することにより、再生態様情報の取り出しを困難にして、不正使用防止効果をさらに高めることができる。

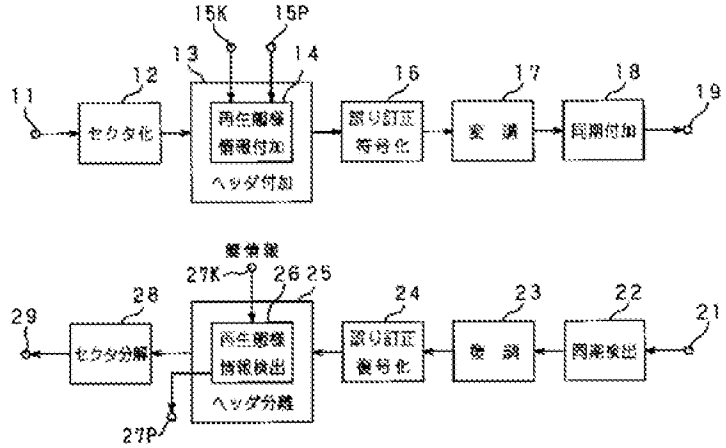
【００４３】これは、暗号化されていない再生態様情報を所定の位置指定情報により指定される位置に配置することでも、再生態様情報を容易に取り出せないようにし、再生態様情報の改変による不正な使用等を防止できる。

【図面の簡単な説明】

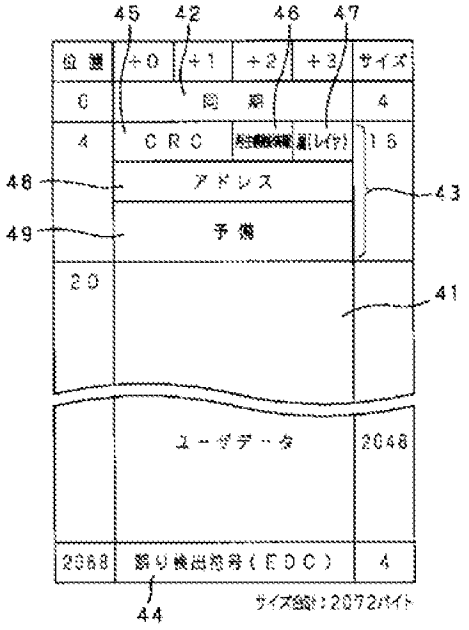
【図１】本発明の実施の形態が適用可能な構成の一例を示すブロック図である。
【図２】セクタフォーマットの一例を示す図である。
【図３】再生態様情報の一例を示す図である。
【図４】暗号化のためのデータ変換回路の具体例を示す図である。
【図５】暗号化のためのデータ変換回路の他の具体例を示す図である。
【図６】データ記録媒体の一例を示す図である。
【図７】再生態様情報の記録位置をポインタにより指定する一例を示す図である。
【図８】アナログビデオ信号に再生態様情報を付加した具体例を説明するための図である。
【符号の説明】

１２　セクタ化回路
１３　ヘッダ付加回路
１４　再生態様情報付加回路
１５Ｋ、２７Ｋ　鍵情報入力端子
１６　誤り訂正符号化回路
１７　変調回路
１８　同期付加回路
２２　同期分離回路
２３　復調回路
２４　誤り訂正復号化回路
２５　ヘッダ分離回路
２６　再生態様情報検出回路
２８　セクタ分解回路

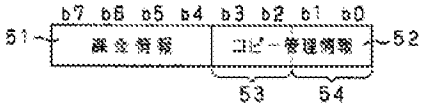
【図１】



【図２】

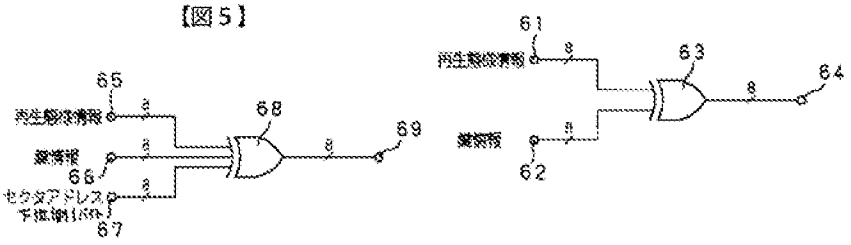


【図３】

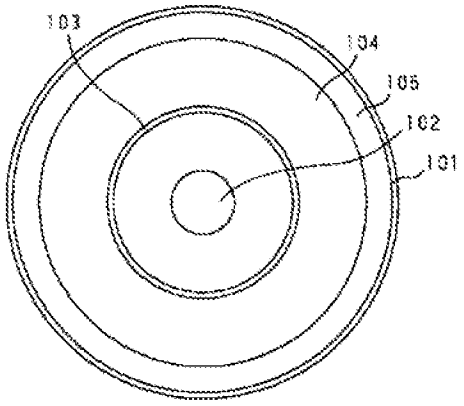


【図４】

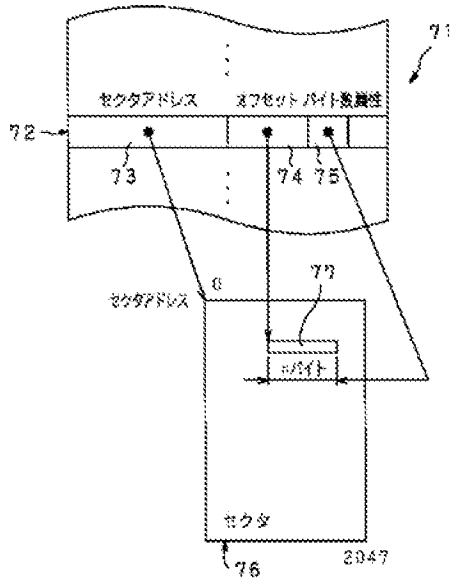
【図５】



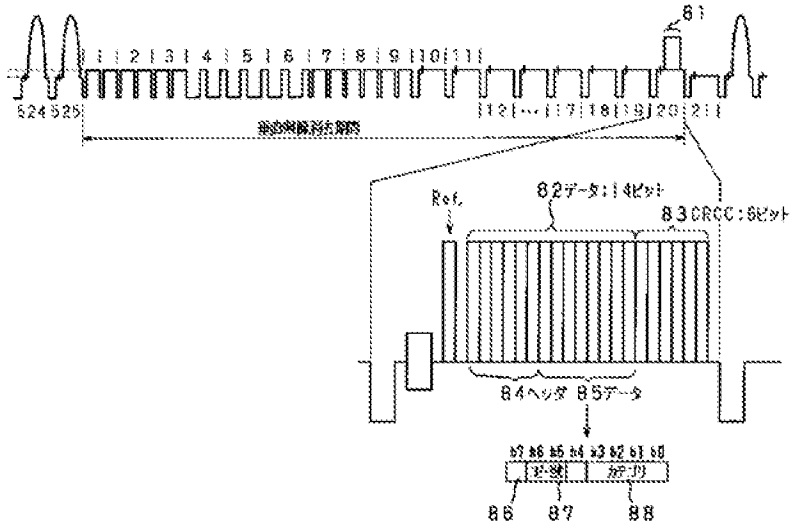
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者　川嶋　功
東京都品川区北品川6丁目7番35号　ソニー株式会社内

(72)発明者　米山　重之
東京都品川区北品川6丁目7番35号　ソニー株式会社内